DOE CYBERSECURITY:

CORE COMPETENCY TRAINING REQUIREMENTS

Key Cybersecurity Role: **Information System Owner**

Role Definition: The Information System Owner (also referred to as System Owner) is the individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of an information system. The System Owner is a key contributor in developing system design specifications to ensure the security and user operational needs are documented, tested, and implemented.

Competency Area: **Data Security**

Functional Requirement: **Design**

Competency Definition: Refers to the application of the principles, policies, and procedures necessary to ensure the confidentiality, integrity, availability, and privacy of data in all forms of media (i.e., electronic and hardcopy) throughout the data life cycle.

Behavioral Outcome: The System Owner will understand the policies and procedures required to protect all categories of information as well as have a working knowledge of data access controls required to ensure the confidentiality, integrity, and availability of information. He/she will apply this knowledge during all phases of the System Development Life Cycle (SDLC).

Training concepts to be addressed at a minimum:

- Identify and document the appropriate level of protection for data, including use of encryption.
- Specify data and information classification, sensitivity, and need-to-know requirements by information type on a system in terms of its confidentiality, integrity, and availability. Utilize DOE M 205.1-5 to determine the information impacts for unclassified information and DOE M 205.1-4 to determine the Consequence of Loss for classified information.
- Create authentication and authorization system for users to gain access to data based on assigned privileges and permissions.
- Develop acceptable use (e.g., personal use of IT policy; waste, fraud, and abuse policy, etc.) procedures in support of the data security policies.
- Identify the minimum security controls based on the system categorization. Develop or identify additional security controls based on the Consequence of Loss or Impact and the perceived risk of compromise to the data introduced by the data's logical, operational, or physical environment.
- Develop media sanitization (clearing, purging, or destroying) and reuse procedures.
- Develop and document processes, procedures, and guidelines for complying with protection requirements (e.g., e-mail labels, media labels, etc.), control procedures (e.g., discretionary access control, need-to-know sharing, etc.), incident management reporting, remote access requirements, system management and use of encryption.

Training Evaluation Criteria: **Demonstrate**
Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge
Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials
Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **detailed** knowledge of DOE/Risk Management Implementation Plans (RMIPs), and Operating Unit policies, requirements, and procedures
- Demonstrate a **detailed** ability to synthesize data management policies and procedures based on the information owner's requirements and DOE/RMIP and Operating Unit policies, requirements, and procedures.
- Demonstrate a **functional** ability to devise acceptable use policy for the system from DOE/RMIP, Operating Unit, and Information Owner's policies and requirements
- Demonstrate a **functional** ability to identify and implement minimum security controls based on DOE/RMIP, Operating Unit, and Information Owner's policies and requirements

Competency Area: **Information Technology (IT) Systems Operations and Maintenance**

Functional Requirement: **Design**

Competency Definition: Refers to the ongoing application of principles, policies, and procedures to maintain, monitor, control, and protect IT infrastructure and the information residing on such infrastructure during the operations phase of an IT system or application. Individuals with these functions perform a variety of data collection, analysis, reporting and briefing activities associated with security operations and maintenance to ensure that the organizational security policies are implemented and maintained on information systems.

Behavioral Outcome: The System Owner will understand the policies, procedures, and controls required to protect IT infrastructure and data to include technical, operational, and administrative security controls as mandated by Departmental/RMIP standards. He/she will apply this knowledge during all phases of the SDLC.

Training concepts to be addressed at a minimum:

- Develop personnel, application, middleware, operating system, hardware, network, facility, and egress security controls as required by design specifications.
- Develop security monitoring, test scripts, test criteria, and testing procedures.
- Develop security administration change management procedures to ensure that security policies and controls remain effective following a change to include identification of roles and responsibilities for change approval/disapproval.
- Develop role-based access, based on the concept of least privilege.

Training Evaluation Criteria: **Demonstrate**
Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge
Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials
Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **detailed** knowledge of DOE/RMIP, and Operating Unit policies, requirements, and procedures
- Demonstrate a **functional** knowledge of configuration management and control principles and processes
- Demonstrate a **functional** knowledge of evaluation methodologies, processes, and reporting
- Demonstrate a **functional** knowledge of methods and technologies to provide capabilities for monitoring and reporting on network/system operation and vulnerabilities
- Demonstrate a **general** knowledge of role responsibilities and rights and privileges required to perform the role.
- Demonstrate a **functional** knowledge of configuration management and control methodologies and procedures

Competency Area: **Information Technology (IT) Systems Operations and Maintenance**

Functional Requirement: **Implement**

Competency Definition: Refers to the ongoing application of principles, policies, and procedures to maintain, monitor, control, and protect IT infrastructure and the information residing on such infrastructure during the operations phase of an IT system or application. Individuals with these functions perform a variety of data collection, analysis, reporting and briefing activities associated with security operations and maintenance to ensure that the organizational security policies are implemented and maintained on information systems.

Behavioral Outcome: The System Owner will understand the policies, procedures, and controls required to protect IT infrastructure and data to include technical, operational, and administrative security controls as mandated by Departmental/RMIP standards. He/she will apply this knowledge during all phases of the SDLC.

Training concepts to be addressed at a minimum:

- Collaborate with technical support, incident management, and security engineering teams to develop, implement, control, and manage new security administration technologies as they pertain to systems for which the system owner is responsible.
- Monitor vendor agreements and Service Level Agreements (SLA) to ensure that contract and performance measures are achieved.
- Create a Plan of Actions and Milestones (POA&M) for correction of vulnerabilities and compensation for risks or threats.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **detailed** knowledge of DOE/RMIP, and Operating Unit policies, requirements, and procedures
- Demonstrate a **functional** knowledge of contract oversight and management processes and procedures
- Demonstrate a **functional** knowledge of performance measures applicable to system operation and contract oversight
- Demonstrate a **functional** knowledge of POA&M requirements and processes promulgated by the DOE/RMIP and Operating Unit

Competency Area: **Network and Telecommunications Security and Remote Access**

Functional Requirement: **Design**

Competency Definition: Refers to application of the principles, policies, and procedures involved in ensuring the security of basic network and telecommunications services and data and in maintaining the hardware layer on which the data resides. Examples of these practices include perimeter defense strategies, defense-in-depth strategies, and data encryption techniques.

Behavioral Outcome: The System Owner will understand the policies, procedures, and controls required to protect network and telecommunication services to include technical, operational, and administrative security controls as mandated by Departmental/RMIP standards. He/she will apply this knowledge during all phases of the SDLC.

Training concepts to be addressed at a minimum:

- Develop processes and procedures for protecting telecommunications networks against unauthorized access and wiretapping (e.g., protected distribution systems, transmission encryption, locked telephone closets, etc.).
- Develop process for interconnecting information systems based on identifying organizational needs, associated risks, and controlled interface requirements
- Develop effective network domain security controls in accordance with organizational, network and host-based policies.
- Develop wireless technology processes, guidelines, and procedures in accordance with Departmental directives and applicable RMIPs.
- Develop and document processes, procedures, and guidelines related to P2P networking commensurate with the level of security required for the organization's environment and specific

needs *and* in accordance with Departmental directives and applicable RMIPs.

- Develop processes, procedures, and identify minimum security controls for External Information Systems and portable/mobile devices. This encompasses security controls for these systems and devices operating in a standalone operation and operating within the proximity of or connected to systems accredited for storing/ processing SUI or classified information.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **detailed** knowledge of DOE/RMIP, and Operating Unit policies, requirements, and procedures
- Demonstrate a **functional** knowledge of project management principles and activities
- Demonstrate a **functional** knowledge of other security disciplines that impact cybersecurity
- Demonstrate a **functional** ability to identify and manage interfaces with other security functions and mission implementation functions
- Demonstrate a **detailed** knowledge of technical specification writing
- Demonstrate a **detailed** ability to analyze policy, control statements, standards, guidance, and regulations for the development of procedures and control implementations
- Demonstrate a **detailed** knowledge of threats and vulnerabilities to evaluate the potential impact and related risk to an individual system and its support infrastructure
- Demonstrate a **detailed** ability to evaluate the applicability of threats and vulnerabilities to networks/information systems
- Demonstrate a **functional** knowledge of design documentation and configuration control during the development phase

Competency Area: **Network and Telecommunications Security and Remote Access**

Functional Requirement: **Implement**

Competency Definition: Refers to application of the principles, policies, and procedures involved in ensuring the security of basic network and telecommunications services and data and in maintaining the hardware layer on which the data resides. Examples of these practices include perimeter defense strategies, defense-in-depth strategies, and data encryption techniques.

Behavioral Outcome: The System Owner will understand the policies, procedures, and controls required to protect network and telecommunication services to include technical, operational, and administrative security controls as mandated by Departmental/RMIP standards. He/she will apply this knowledge during all phases of the SDLC.

Training concepts to be addressed at a minimum:

- Document interconnected system specifics (e.g., purpose, risk, information types, technical implementation, etc.) in accordance with Departmental directives and applicable RMIPs.
- Implement policies, procedures, and minimum security controls for the use of External Information Systems, wireless information technology, and portable/mobile devices in accordance with Departmental directives and applicable RMIPs.
- Implement policies and procedures related to P2P networking in accordance with Departmental directives and applicable RMIPs.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **detailed** knowledge of DOE/RMIP, and Operating Unit policies, requirements, and procedures
- Demonstrate a **functional** knowledge of System Security Plan creation/development
- Demonstrate a **functional** knowledge of remote access methods and technologies
- Demonstrate a **functional** ability to describe control implementation for secure use of local and remote access technologies and methods

Competency Area: **Personnel Security**

Functional Requirement: **Design**

Competency Definition: Refers to the knowledge of human resource selection methods and controls used by an organization to help deter willful acts of security breaches such as theft, fraud, misuse, and noncompliance. These controls include organization/functional design elements such as separation of duties, job rotation, and classification.

Behavioral Outcome: The System Owner will be knowledgeable of Personnel Security policies and procedures and will coordinate with the appropriate security offices to ensure that personnel security access controls are implemented as required by the system organization/functional design specifications and as mandated by Departmental/RMIP standards. This individual will also ensure that personnel access security controls such as restricted access based on appropriate security clearances and need-to-know authorizations as well as job roles and/or duties are incorporated in all phases of the SDLC.

Training concepts to be addressed at a minimum:

- Establish personnel security processes and procedures for individual job roles.

- Establish procedures for coordinating with other organizations to ensure that common processes are aligned.
- Establish personnel security rules and procedures to which external suppliers (e.g., vendors, contractors) must conform.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **general** knowledge of DOE/SDM and Operating Unit personnel security policies, requirements, and procedures
- Demonstrate a **functional** knowledge of DOE/RMIP and Operating Unit personnel security controls
- Demonstrate a **general** knowledge of personnel screening policies and requirements
- Demonstrate a **general** knowledge of system security role's security responsibilities

Competency Area: **Physical and Environmental Security**

Functional Requirement: **Design**

Competency Definition: Refers to the knowledge of controls and methods used to protect an organization's operational environment including personnel, computing equipment, data, and physical facilities. This concept also refers to the methods and controls used to proactively protect an organization from natural or man-made threats to physical facilities, as well as physical locations where IT equipment is located (e.g., central computing facility).

Behavioral Outcome: The System Owner will be knowledgeable of Physical Security policies and procedures and will coordinate with the appropriate security offices to ensure that physical controls are implemented as required by the system organization/functional design specifications and as mandated by Departmental/RMIP standards. This individual will use this knowledge to assist with identifying and mitigating environmental security threats, both natural and man-made, to computing equipment and facilities during all phases of the SDLC.

Training concepts to be addressed at a minimum:

- Identify the physical security program requirements and specifications in relationship to system security goals.
- Develop policies and procedures for identifying and mitigating physical and environmental threats (to include TEMPEST concerns) to information assets, personnel, facilities, and equipment.

- Develop a physical security and environmental security plan, including security test plans and contingency plans, in coordination with other security planning functions.
- Develop countermeasures against identified risks and vulnerabilities.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **general** knowledge of DOE/SDM and Operating Unit physical and environmental security policies, requirements, and procedures
- Demonstrate a **functional** knowledge of DOE/RMIP and Operating Unit physical and environmental security controls
- Demonstrate a **general** knowledge of physical/environmental risk and vulnerability assessment procedures
- Demonstrate a **functional** ability to analyze cybersecurity controls and physical security policy to identify common controls for information systems
- Demonstrate a **general** knowledge of methods for mitigating physical proximity threats for system components, personnel, and facilities.
- Demonstrate a **general** knowledge of methods for mitigating physical proximity threats for system components, personnel, and facilities.

Competency Area: **Procurement**

Functional Requirement: **Manage**

Competency Definition: Refers to the application of principles, policies, and procedures required to plan, apply, and evaluate the purchase of IT products or services—including "risk-based" pre-solicitation, solicitation, source selection, award, and monitoring, disposal, and other post-award activities. Procurement activities may consist of the development of procurement and contract administration documents that include, but are not limited to, procurement plans, estimates, requests for information, requests for quotes, requests for proposals, statements of work, contracts, cost-benefit analyses, evaluation factors for award, source selection plans, incentive plans, service level agreements (SLA), justifications required by policies or procedures, and contract administration plans.

Behavioral Outcome: The System Owner will be knowledgeable of the principles, policies, and procedures required for the procurement of IT products. This individual will ensure that operational, functional, and risk-based security specifications are included in all pertinent procurement documents to include requests for bids, statements of work, evaluation criteria, acquisitions plans, etc.

Training concepts to be addressed at a minimum:

- Collaborate with various stakeholders (including internal clients and purchasing organizations, lawyers, Chief Information Officers, Chief Information Security Officers, cybersecurity professionals, privacy professionals, security engineers, suppliers, etc.) on the procurement of IT security products and services.
- Ensure the inclusion of risk-based cybersecurity requirements in acquisition plans, cost estimates, statements of work, contracts, and evaluation factors for award, service level agreements, and other pertinent procurement documents.
- Ensure that investments are aligned with organizational architecture and security requirements.
- Conduct detailed IT investment reviews and security analyses and review IT investment business cases for security requirements.
- Specify policies for use of government information by vendors and/or partners and connection requirements and acceptable use policies for vendors that connect to government networks.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **functional** knowledge of DOE/RMIP and Operating Unit policy, standards, and guidance and regulations
- Demonstrate a **general** knowledge of procurement processes sufficient to identify cybersecurity requirements in appropriate format for procurements
- Demonstrate a **functional** knowledge of capital planning and investment control (CPIC)
- Demonstrate a **detailed** ability to analyze cybersecurity costs in relation cybersecurity control requirements and the mission and goals of the SDM organization and Operating Unit mission statements
- Demonstrate a **functional** knowledge of project management principles and activities
- Demonstrate a **functional** knowledge of documents required to adequately specify cybersecurity requirements for contracting activities
- Demonstrate a **functional** knowledge of the DOE/SDM and Operating Unit Enterprise Architecture(s)
- Demonstrate a **functional** knowledge of technical architecture design as it relates to the implementation of cybersecurity within the DOE/SDM and Operating Unit Enterprise Architecture(s)

Competency Area: **Security Risk Management**

Functional Requirement: **Design**

Competency Definition: Refers to the knowledge of policies, processes, and technologies used to create

a balanced approach to identifying and assessing risks to information assets, personnel, facilities, and equipment, and to manage mitigation strategies that achieve the security needed at an affordable cost.

Behavioral Outcome: The System Owner will be knowledgeable of organizational risk management policies, procedures, and mitigation strategies and will apply this knowledge when determining risk-based security specifications during system organization/functional design development, testing, maintenance, and disposition.

Training concepts to be addressed at a minimum:

- Develop a risk assessment process for identifying and assessing environmental (operational, logical, or physical) and system risks to information assets, personnel, facilities, and equipment and mitigating those risks
- Assist with developing a process for determining the security significance of proposed environmental and system changes and the resulting reaccreditation requirements.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **functional** knowledge of the DOE/RMIP policies and procedures for evaluating and managing risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation
- Demonstrate a **functional** knowledge of methodologies and techniques for evaluating risks
- Demonstrate a **functional** knowledge of risk management techniques
- Demonstrate a **detailed** ability to identify applicability of risk management techniques
- Demonstrate a **detailed** knowledge of potential changes in configuration that may impact security function/control effectiveness
- Demonstrate a **functional** knowledge of costs associated with security implementation
- Demonstrate a **functional** knowledge of methods of control implementations and the associated risks
- Demonstrate a **functional** ability to analyze DOE/RMIP policies and procedures for evaluating and managing risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation and identify methods, processes, and steps to implement them

Competency Area: **System and Application Security**

Functional Requirement: **Design**

Competency Definition: Refers to the knowledge of principles, practices, and procedures required to integrate information security into an IT system or application during the SDLC. The goal of this activity is to ensure that the operation of IT systems and software does not present undue risk to the organization and information assets. Supporting activities include risk assessment, risk mitigation, security control selection, implementation and evaluation, certification and accreditation (C&A), and software security standards compliance.

Behavioral Outcome: The System Owner will understand SDLC policies and processes and will integrate applicable risk-based information security requirements, controls, configurations, and processes during the application/system design process.

Training concepts to be addressed at a minimum:

- Specify the organizational and IT system and application security policies, standards, and best practices.
- Integrate applicable information security requirements, controls, processes, and procedures into information system and application design specifications in accordance with Departmental and/or RMIP established standards, policies, procedures, guidelines, directives, and regulations and laws (statues).
- Specify minimum security configurations for the IT system or application as required by Departmental directives and applicable RMIPs.
- Identify standards against which to engineer the IT system or application.
- Develop processes and procedures to mitigate the introduction of vulnerabilities during the engineering process.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **functional** knowledge of the DOE/RMIP policies and procedures for evaluating and managing risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation
- Demonstrate a **functional** knowledge of DOE/RMIP/Operating Unit policies, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **functional** knowledge of the SDLC process and available cybersecurity standards and guidelines
- Demonstrate a **functional** knowledge of methods for allocation of hardware and software to identify system components
- Demonstrate a **functional** ability to structure security implementations into the IT SDLC process for the Operating Unit

- Demonstrate a **functional** knowledge of secure system development processes and tools
- Demonstrate a **functional** knowledge of project management principles and activities

Competency Area: **System and Application Security**

Functional Requirement: **Implement**

Competency Definition: Refers to the knowledge of principles, practices, and procedures required to integrate information security into an IT system or application during the SDLC. The goal of this activity is to ensure that the operation of IT systems and software does not present undue risk to the organization and information assets. Supporting activities include risk assessment, risk mitigation, security control selection, implementation and evaluation, certification and accreditation (C&A), and software security standards compliance.

Behavioral Outcome: The System Owner will understand SDLC policies and processes and will integrate applicable risk-based information security requirements, controls, configurations, and processes during the application/system design and validation lifecycle phases.

Training concepts to be addressed at a minimum in course curricula:

- Document POA&Ms as required for security controls that have not been implemented correctly.
- Initiate the revision of security controls that did not meet expectations during the certification phase via the SDLC process.

Training Evaluation Criteria: **Demonstrate**

Methods of Demonstration: **Examination; Simulation; Desk Top Analysis**

Level of Demonstration:

General – Demonstrates an overall understanding of the purpose and objectives of the process/topic adequate to discuss the subject or process with individuals of greater knowledge

Functional – Demonstrates an understanding of the individual parts of the process/topic and the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials

Detailed – Demonstrates an understanding of the inner workings of individual parts of the process/topic and comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance

- Demonstrate a **functional** knowledge of the DOE/RMIP policies and procedures for evaluating and managing risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation
- Demonstrate a **functional** knowledge of DOE/RMIP/Operating Unit policies, processes, procedures, directives, regulations, and public laws (statutes)
- Demonstrate a **functional** ability to evaluate assessment results and determine adequacy of control implementation
- Demonstrate a **detailed** ability to analyze controls implementation for evaluating compliance with the SSP
- Demonstrate a **detailed** ability to devise adequate implementations of controls
- Demonstrate a **functional** knowledge of the purpose of POA&Ms and the procedures for creating and coordinating a POA&M